JC19 Rec'd PCT/PTO 17 JUL 2001

FORM PTO-1390 (Modified) (REV 11-98) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: **520.1002**

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR): **To Be Assigned 09/889420**

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP99/09844	**9 December 1999**	**18 January 1999**

TITLE OF INVENTION

DEVICE AND METHOD FOR SYNCHRONIZING VOLTAGE CIPHERING MACHINE IN ATM NETWORKS

APPLICANT(S) FOR DO/EO/US

Ulrich HEISTER

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ A copy of the International Search Report (PCT/ISA/210).
8. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
9. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 20 below concern document(s) or information included:

13. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
16. ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
17. ☐ A substitute specification.
18. ☐ A change of power of attorney and/or address letter.
19. ☒ Certificate of Mailing by Express Mail
20. ☒ Other items or information:

- **Letter re: Priority**
- **Postcard**

JC17 Rec'd PCT/PTO 17 JUL 2001

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR)	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/889420 To Be Assigned	PCT/EP99/09844	520.1002

21. The following fees are submitted:.

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :

		CALCULATIONS PTO USE ONLY
☐	Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO and International Search Report not prepared by the EPO or JPO	$1,000.00
☒	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but Internation Search Report prepared by the EPO or JPO	$860.00
☐	International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO	$710.00
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provisions of PCT Article 33(1)-(4)	$690.00
☐	International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(1)-(4)	$100.00

ENTER APPROPRIATE BASIC FEE AMOUNT =	$860.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).	$0.00	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	7 - 20 =	0	x $18.00	$0.00	
Independent claims	2 - 3 =	0	x $80.00	$0.00	
Multiple Dependent Claims **(check if applicable)**.			☐	$0.00	
TOTAL OF ABOVE CALCULATIONS =				$860.00	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable)**.			☐	$0.00	
SUBTOTAL =				$860.00	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). +				$0.00	
TOTAL NATIONAL FEE =				$860.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			☐	$0.00	
TOTAL FEES ENCLOSED =				$860.00	
				Amount to be: refunded	$
				charged	$

☒ A check in the amount of **$860.00** to cover the above fees is enclosed.

☐ Please charge my Deposit Account No. in the amount of to cover the above fees.
A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **50-0552** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

William C. Gehris
Davidson, Davidson & Kappel, LLC
485 Seventh Avenue, 14th Floor
New York, NY 10018

23280
PATENT TRADEMARK OFFICE

SIGNATURE

Cary S. Kappel
NAME

36,561
REGISTRATION NUMBER

July 17, 2001
DATE

09/889420
JC17 Rec'd PCT/PTO 17 JUL 2001

[520.1002]

UNITED STATES PATENT AND TRADEMARK OFFICE

Re:	Application of:	Ulrich HEISTER
	Serial No.:	To Be Assigned
	International Application No.:	PCT/EP99/09844
	Filed:	Herewith
	For:	DEVICE AND METHOD FOR SYNCHRONIZING VOLTAGE CIPHERING MACHINE IN ATM NETWORKS

BOX PCT
Asst. Commissioner for Patents
Washington, D.C. 20231

July 17, 2001

PRELIMINARY AMENDMENT

Sir:

Applicants request that the following Amendments be made in the above-identified matter prior to examination thereof:

IN THE TITLE

Please amend the title to read as follows: --DEVICE AND METHOD FOR SYNCHRONIZING STREAM ENCRYPTORS IN ATM NETWORKS--.

IN THE SPECIFICATION

Before paragraph [0001], please change the heading "Specification" to --Field of the Invention--.

Before paragraph [0002], please insert the heading: --Related Technology--.

Before paragraph [0007], please insert heading: --Summary of the Invention--.

Please amend paragraph [0007] to read as follows:

[0007] An object of the present invention is to provide a reliable method for synchronizing stream decryptors which does not require additional capacity and can be implemented with a small outlay.

Please amend paragraph [0008] to read as follows:

[0008] The present invention allocates a state automaton to the stream encryptor and to the at least one stream decryptor, respectively, it being possible for the state automaton to be advanced from ATM cell to ATM cell, and the respective state, besides the secret key, being used for generating the variable key.

Please amend paragraph [0009] to read as follows:

[0009] In this context, provision can be made for the state to be able to be fed to a device for generating a function as a function of the state and of the secret key, the device being designed for controlling the pseudo-random generator.

Please amend paragraph [0011] to read as follows:

[0011] In an embodiment according to the present invention, in the stream encryptor, the secret key of the destination of the specific transmitted ATM cell and the respective state are used for generating the variable key, and the state automatons of the stream encryptor and of the stream decryptors can be advanced independently of the destination of the specific ATM cell. In this context, each ONT (optical network termination) has a secret key, the OLT (optical line termination) has the secret keys of all ONTs.

Please amend paragraph [0012] to read as follows:

[0012] In the method according to the present invention the variable key depends, moreover, on the state of a state automaton which is allocated to the stream encryptor and to the at least one stream decryptor and which is advanced from ATM cell to ATM cell. In this context, provision may be made for the advance of the state automaton to be derived in response to the detection of a cell boundary by comparing a check sequence computed from the header to a check sequence which is also transmitted in the header of the cell. This does not involve any additional outlay because devices for cell boundary detection are needed in the receivers anyway.

Please amend paragraph [0013] to read as follows:

[0013] In an embodiment of the method according to the present invention an input variable for the respective pseudo-random generator is generated from the secret key and the respective state with the aid of a predefined function.

Please amend paragraph [0014] to read as follows:

[0014] The method according to the present invention may be advantageously applied where several receivers which each have a stream decryptor are connected to the transmission channel, and, in this connection, headers of the ATM cells contain information on which receivers are the destinations of the ATM cells, because the secret key of the stream decryptor at the respective destination is taken as the basis for generating the variable key in the stream encryptor and because the state automatons allocated to the stream encryptor and to the stream decryptors are advanced in response to each transmitted ATM cell.

Before paragraph [0015], please insert the heading:

--Brief Description of the Drawings--.

Please amend paragraph [0015] to read as follows:

[0015] Exemplary embodiments of the present invention are elaborated upon below with reference to the drawings, in which:

Please amend paragraph [0016] to read as follows:

[0016] Figure 1 shows a schematic representation of an ATM network including a transmitter and two receivers; and

Figure 2 shows a schematic representation of a prior art method for cell boundary detection.

Before paragraph [0017], please insert the heading: --Detailed Description--.

Please amend paragraph [0018] to read as follows:

[0018] A prior art device for cell boundary detection is schematically shown in Fig. 2; 40 bits being tapped in each case from the cell stream supplied via 2 (in the Figure, one arrow represents 4 bits). Via bits 9 through 40, a HEC is generated at 13 in the same manner as in the transmitter, the HEC being compared to the preceding bits 1 through 8 in an 8-bit comparator 14. In the case of equality, a signal is emitted at 15 which signifies the detection of a valid header. staggered by a certain angular value between adjacent intermediate walls 6 to prevent a continuous electric arc in the current-limiting event.

Page 6, first line, please change : "What is claimed is" to --WHAT IS CLAIMED IS--.

IN THE CLAIMS:

Please cancel claims 1-7 as presented in the underlying International Application No. PCT/EP99/09844, as well as the revised claims 1-3 annexed to the International Preliminary Examination Report (a translation of which claims is submitted herewith), and add new claims 8-14 as follows:

--8. (new) An apparatus for synchronizing at least one stream decryptor connected to a transmission channel for ATM cells at a receiver end, a stream encryptor being disposed in the transmission channel at a transmitter end, the device comprising:

a first pseudo-random generator associated with the stream encryptor for generating a respective first variable key associated with each of the at least one stream decryptor using a respective secret key associated with each of the at least one stream decryptor;

a respective second pseudo-random generator associated each of the at least one stream decryptor for generating a respective second variable key using the respective secret key, each of the respective second variable key being identical to the associated respective first variable key;

a respective device for cell boundary detection associated with each of the at least one stream decryptor; and

a respective state automaton associated with the stream encryptor and each of the at least one stream decryptor, a respective state of each respective state automaton associated with the at least one stream decryptor being capable of being advanced by the respective device for cell boundary detection, each of the respective states being used for generating the respective variable key.

9. (new) The apparatus as recited in claim 8 wherein the respective state of each state automaton is capable of being fed to a respective device for generating a predefined function using the respective state and the respective secret key, each of the device for generating a predefined function being capable of controlling the respective pseudo-random generator.

10. (new) The apparatus as recited in claim 8 wherein the at least one stream decryptor includes a plurality of stream decryptors, a respective receiver being associated with each of the plurality of stream decryptors, each of the receivers being connected to the transmission channel, a respective header of each of the ATM cells including respective information identifying a respective destination receiver of the receivers;

wherein the stream encryptor is capable of generating the respective first variable key using the respective secret key associated with the respective destination receiver of a respective transmitted ATM cell and the respective state; and

wherein each of the state automatons are capable of being advanced independently of the respective destination receiver.

11. (new) A method for synchronizing at least one stream decryptor connected to a transmission channel for ATM cells at a receiver end, a stream encryptor being disposed in the transmission channel at a transmitter end, the method comprising:

generating a respective first variable key associated with each of the at least one stream decryptor using a respective secret key associated with each of the at least one stream decryptor and a first pseudo-random generator associated with the stream encryptor;

generating a respective second variable key associated with each of the at least one stream decryptor using the respective secret key and a respective second pseudo-random generator associated with the respective stream decryptor, each respective second variable key being identical the respective first variable key; and

advancing on a per-ATM cell basis a respective state of a respective state automaton associated with the stream encryptor and each of the at least one stream decryptor, each of the first and second variable keys being a function of the respective state.

12. (new) The method as recited in claim 11 wherein the advancing of the respective state associated with each of the at least one stream decryptor is performed in response to a detecting of a respective ATM cell boundary, the detecting being performed by comparing a check sequence computed from a respective header of the ATM cell to a check sequence transmitted in the header.

13. (new) The method as recited in claim 11 further comprising generating a respective input variable for each of the pseudo-random generator using the respective secret key, the respective state, and a respective predefined function.

14. (new) The method as recited in claim 11 wherein the at least one stream decryptor includes a plurality of stream decryptors, a respective receiver being associated with each of the plurality of stream decryptors, each of the receivers being connected to the transmission channel, a respective header of each of the ATM cells including respective information identifying a respective destination receiver of the receivers;

generating each of the first and second variable keys using the respective secret key of the respective stream decryptor associated with each of the destination receivers; and

advancing the respective state of each of the state automatons in response to a transmission of an ATM cell.--.

IN THE ABSTRACT:

Please replace the Abstract of record with the following new Abstract:

--A device and a method for synchronizing at least one stream decryptor connected to a transmission channel for ATM cells at the receiver end, with a stream encryptor arranged in the transmission channel at the transmitter end. The stream encryptor and each stream decryptor each have a pseudo-random generator which generates a variable key which is identical at the transmitter and at the receiver end. The stream decryptor(s) are each allocated a device for cell boundary detection. The stream encryptor and the stream decryptor(s) are each allocated a state automaton, it being possible for the state automaton(s) of the stream decryptors to be advanced by the respective devices for cell boundary detection. The respective state and the respective secret key are used for generating the variable key.--.

REMARKS

Consideration of this application, as amended, is respectfully requested.

Support for all new claims is found in the specification as originally filed. It is respectfully submitted that no new matter has been added.

Applicants believe that no fees are due as a result of this amendment. In the event of a fee discrepancy, please charge our Deposit Account No. 50-0552.

Respectfully submitted,

DAVIDSON, DAVIDSON & KAPPEL, LLC

By: _____

Cary S. Kappel
Reg. No. 36,561

Davidson, Davidson & Kappel, LLC
485 Seventh Avenue - 14th Floor
New York, New York 10018
(212) 736-1940

"Express Mail" mailing label no. EL 825523305 US
Date of deposit: July 17, 2001
I hereby certify that this correspondence and/or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above in an envelope addressed to "Commissioner of Patents and Trademarks, Washington, DC 20231"

DAVIDSON, DAVIDSON & KAPPEL, LLC

BY: Randolph McQueen
Randolph McQueen

Application of: Ulrich Heister
International Application No. PCT/EP99/09844
Filed Herewith

VERSION OF SPECIFICATION AND CLAIMS AMENDMENTS
WITH MARKINGS TO SHOW CHANGES MADE

IN THE TITLE:

DEVICE AND METHOD FOR SYNCHRONIZING STREAM ENCRYPTORS [VOLTAGE CIPHERING MACHINE] IN ATM NETWORKS

IN THE SPECIFICATION:

Page 1, before paragraph [0001]: [Specification] Field of the Invention.

Page 1, before paragraph [0002]: --Related Technology--.

Page 2, before paragraph [0007]: --Summary of the Invention--.

Page 2, paragraph [0007]:
[0007] [The] An object of the present invention is to [specify] provide a reliable method for synchronizing stream decryptors which does not require additional capacity and can be implemented with [the smallest possible] a small outlay.

Page 2, paragraph [0008]:
[0008] [In the device according to the present invention, this object is achieved by allocating] The present invention allocates a state automaton to the stream encryptor and to the at least one stream decryptor, respectively, it being possible for the state automaton to be advanced from

ATM cell to ATM cell, and the respective state, besides the secret key, being used for generating the variable key.

Page 2, paragraph [0009]:

[0009] In this context, provision can be made [in a preferred embodiment] for the state to be able to be fed to a device for generating a function as a function of the state and of the secret key, the device being designed for controlling the pseudo-random generator.

Page 3, paragraph [0011]:

[0011] [The device according to the present invention can, in principle, be already used in the case of a transmission between a transmitter and a receiver. However, a particularly advantageous further refinement consists in that] In an embodiment according to the present invention, in the stream encryptor, the secret key of the destination of the specific transmitted ATM cell and the respective state are used for generating the variable key, and [in that] the state automatons of the stream encryptor and of the stream decryptors can be advanced independently of the destination of the specific ATM cell. In this context, each ONT (optical network termination) has a secret key, the OLT (optical line termination) has the secret keys of all ONTs.

Page 3, paragraph [0012]:

[0012] [The objective is achieved in] In the method according to the present invention [in that] the variable key depends, moreover, on the state of a state automaton which is allocated to the stream encryptor and to the at least one stream decryptor and which is advanced from ATM cell to ATM cell. In this context, provision [is preferably] may be made for the advance of the state automaton to be derived in response to the detection of a cell boundary by comparing a check sequence computed from the header to a check sequence which is also transmitted in the header of the cell. This does not involve any additional outlay because devices for cell boundary detection are needed in the receivers anyway.

Page 3, paragraph [0013]:

[0013] [An advantageous] In an embodiment of the method according to the present invention [consists in that] an input variable for the respective pseudo-random generator is generated from the secret key and the respective state with the aid of a predefined function.

Page 3, paragraph [0014]:

[0014] The method according to the present invention [is] may be [particularly advantageous] advantageously applied [if] where several receivers which each have a stream decryptor are connected to the transmission channel, and, in this connection, headers of the ATM cells contain information on which receivers are the destinations of the ATM cells, because the secret key of the stream decryptor at the respective destination is taken as the basis for generating the variable key in the stream encryptor and because the state automatons allocated to the stream encryptor and to the stream decryptors are advanced in response to each transmitted ATM cell.

Page 4, before paragraph [0015]: --Brief Description of the Drawings--.

Page 4, paragraph [0015]:

[0015] Exemplary embodiments of the present invention are [shown in the drawing on the basis of several Figures and explained in greater detail in the following description] elaborated upon below with reference to the drawings, in which:.

Page 4, paragraph [0016]:

[0016] Figure 1 shows a [detail] schematic representation of an ATM network including a transmitter and two receivers; and

Figure 2 shows a schematic representation of a prior art method for cell boundary detection [which is known per se].

Page 4, before paragraph [0017]: --Detailed Description--.

Page 4, paragraph [0018]:

[0018] A prior art device for cell boundary detection is schematically shown in Fig. 2; 40 bits being tapped in each case from the cell stream supplied via 2 (in the Figure, one arrow represents 4 bits). Via bits 9 through 40, a HEC is generated at 13 in the same manner as in the transmitter, the HEC being compared to the preceding bits 1 through 8 in an 8-bit comparator 14. In the case of equality, a signal is emitted at 15 which signifies the detection of a valid header. staggered by a certain angular value between adjacent intermediate walls 6 to prevent a continuous electric arc in the current-limiting event.

Page 6 first line : --WHAT IS CLAIMED IS--[What is claimed is].

1/PRTS

09/889420
JC17 Rec'd PCT/PTO 17 JUL 2001

DEVICE AND METHOD FOR SYNCHRONISING VOLTAGE CIPHERING MACHINE IN ATM NETWORKS

Specification

[0001] The present invention relates to a device and a method for synchronizing at least one stream decryptor connected to a transmission channel for ATM cells at the receiver end, having a stream encryptor arranged in the transmission channel at the transmitter end, the stream encryptor and stream decryptor(s) each having a pseudo-random generator which generates a variable key stream which is identical at the transmitter and at the receiver ends with the aid of a secret key.

[0002] In broadband ISDN, transmission takes place in asynchronous transfer mode (ATM), the information being packetized into packets of identical length, so-called "ATM cells", hereinafter also called "cells". A cell is composed of a five octet long header and an 48 octet long information field containing the payload. The header of the cell is primarily used for identifying the connection to which this cell belongs. This identification is referred to as Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). This and other information occupy a total of 32 bits in the header and are protected by an eight-bit error-correcting code.

[0003] This error-correcting code, also called HEC (Header Error Control), is able to detect up to three-bit errors and to correct one-bit errors and adjacent double errors. Besides error protection, the HEC is also used for cell boundary detection, which described, inter alia, in Sigmund: "ATM – Die Technik des Breitband-ISDN" [ATM – The Technology of Broadband ISDN], R.v. Decker Publishing House, 2nd edition, 1994.

[0004] A valid header is found if the check sequence computed from these 32 bits coincides with the check sequence which is transmitted in the HEC field. At that point, the synchronization at the receiver end latches. After 53 octets, a valid header is expected again. In order to not interrupt the cell boundary detection process and thus maintaining the ATM cell synchronization, a continuous cell stream is required. ATM cell boundary detection is a very rugged synchronization method.

[0005] In stream encryptors and stream decryptors, a pseudo-random sequence generated by a cryptographically strong pseudo-random generator (PRG) is used as a variable key. Unencrypted data p(t) is modulo-2 added with variable key k(t), resulting in encrypted data c(t). The decryption is then carried out using the same variable key k(t). For generating in

each case the same variable key, the two pseudo-random generators need to be synchronized.

[0006] The use of stream encryptors and stream decryptors in an ATM network and their synchronization is described by Heister U., Killat U.: "Private and Authentic Communication in Passive Optical Networks", International Journal of Network Management, Volume 5, Number 2, March-April 1995. In this connection, it is proposed to transmit an initialization vector for synchronizing the stream decryptor. However, this requires additional transmission capacity.

[0007] The object of the present invention is to specify a reliable method for synchronizing stream decryptors which does not require additional capacity and can be implemented with the smallest possible outlay.

[0008] In the device according to the present invention, this object is achieved by allocating a state automaton to the stream encryptor and to the at least one stream decryptor, respectively, it being possible for the state automaton to be advanced from ATM cell to ATM cell, and the respective state, besides the secret key, being used for generating the variable key.

[0009] In this context, provision can be made in a preferred embodiment for the state to be able to be fed to a device for generating a function as a function of the state and of the secret key, the device being designed for controlling the pseudo-random generator.

[0010] The device according to the present invention can be used both between optical line terminations (OLT) and in the case of optical network terminations (ONT), in each case one OLT and one ONT being provided with a pseudo-random generator and a state automaton. When the system is initialized, all state automatons are set to the same initial state. Each ONT has a secret key.

[0011] The device according to the present invention can, in principle, be already used in the case of a transmission between a transmitter and a receiver. However, a particularly advantageous further refinement consists in that, in the stream encryptor, the secret key of the destination of the specific transmitted ATM cell and the respective state are used for generating the variable key, and in that the state automatons of the stream encryptor and of the stream decryptors can be advanced independently of the destination of the specific ATM cell. In this context, each ONT (optical network termination) has a secret key, the OLT (optical line termination) has the secret keys of all ONTs.

[0012] The objective is achieved in the method according to the present invention in that the variable key depends, moreover, on the state of a state automaton which is allocated to the stream encryptor and to the at least one stream decryptor and which is advanced from ATM cell to ATM cell. In this context, provision is preferably made for the advance of the state automaton to be derived in response to the detection of a cell boundary by comparing a check sequence computed from the header to a check sequence which is also transmitted in the header of the cell. This does not involve any additional outlay because devices for cell boundary detection are needed in the receivers anyway.

[0013] An advantageous embodiment of the method according to the present invention consists in that an input variable for the respective pseudo-random generator is generated from the secret key and the respective state with the aid of a predefined function.

[0014] The method according to the present invention is particularly advantageous if several receivers which each have a stream decryptor are connected to the transmission channel, and, in this connection, headers of the ATM cells contain information on which receivers are the destinations of the ATM cells, because the secret key of the stream decryptor at the respective destination is taken as the basis for generating the variable key in the stream encryptor and because the state automatons allocated to the stream encryptor and to the stream decryptors are advanced in response to each transmitted ATM cell.

[0015] Exemplary embodiments of the present invention are shown in the drawing on the basis of several Figures and explained in greater detail in the following description.

[0016] Figure 1 shows a detail of an ATM network including a transmitter and two receivers; and Figure 2 shows a schematic representation of a method for cell boundary detection which is known per se.

[0017] In Fig. 1, a transmitter 1, which forms part of an otherwise not shown OLT, transmits a stream of ATM cells via an optical network 2 to receivers in ONTs of which only two receivers 3, 4 are shown. Prior to transmission, the playload data of each cell is encrypted using a stream encryptor which is composed of an exclusive OR circuit 5 and a pseudo-random generator 6 which feeds in each case one variable key k1(t), k2(t) to exclusive OR circuit 5 so that playload data p(t) is fed to optical network 2 as encrypted data c(t). Connected in series to and before receivers 3 and 4 are stream decryptors 7, 11; 8, 12 for decryption to which the cell stream is fed via a device 9, 10 for detecting the cell boundaries, respectively, and in which in each case one pseudo-random generator 11, 12 derives a variable key k1(t), k2(t) which is fed to in each case one exclusive OR circuit. The signal

derived by devices 9, 10 indicates the boundary of a cell and is also needed in receivers 3, 4 for evaluating the header.

[0018] A device for cell boundary detection is schematically shown in Fig. 2; 40 bits being tapped in each case from the cell stream supplied via 2 (in the Figure, one arrow represents 4 bits). Via bits 9 through 40, a HEC is generated at 13 in the same manner as in the transmitter, the HEC being compared to the preceding bits 1 through 8 in an 8-bit comparator 14. In the case of equality, a signal is emitted at 15 which signifies the detection of a valid header.

[0019] The stream encryptor and the stream decryptors are each allocated a state automaton 16, 17, 18 which is advanced at the beginning of each cell. The then assumed specific state is fed in each case to a device 19, 20, 21 for computing function values from the state and a secret key. Device 19 is controlled by transmitter 1 in such a manner that a secret key k1 or k2 is used, depending on the destination of the cell. Devices 20 and 21 at the receiver end each receive only one secret key k1 or k2.

[0020] Via the encryption with the key of the respective receiver and by advancing state automatons 16, 17, 18 in response to the transmission of each cell, always the correct variable key k1(t) or k2(t) is used at the respective receiver. The ATM cell boundary detection used for synchronization is a very rugged synchronization method which permits reliable decryption of the transmitted data, using the present invention.

What is claimed is:

1. A device for synchronizing at least one stream decryptor connected to a transmission channel for ATM cells at the receiver end, having a stream encryptor arranged in the transmission channel at the transmitter end, the stream encryptor and the stream decryptor(s) each having a pseudo-random generator which generates a variable key which is identical at the transmitter and at the receiver ends with the aid of a secret key,

wherein the stream encryptor and the at least one stream decryptor are each allocated a device for cell boundary detection and a state automaton, it being possible for the state automaton to be advanced by the device for cell boundary detection, and the respective state, besides the secret key, being used for generating the variable key.

2. The device as recited in Claim 1,

wherein the state can be fed to a device for generating a function as a function of the state and of the secret key, the device being designed for controlling the pseudo-random generator.

3. The device as recited in one of the preceding Claims, several receivers which each have a stream decryptor being connected to the transmission channel, and headers of the ATM cells containing information on which receivers are the destinations of the ATM cells,

wherein the secret key of the destination of the specific transmitted ATM cell and the respective state are used for generating the variable key in the stream encryptor, and the state automatons of the stream encryptor and of the stream decryptors can be advanced independently of the destination of the specific cell.

4. A method for synchronizing at least one stream decryptor connected to a transmission channel for ATM cells at the receiver end, having a stream encryptor arranged in the transmission channel at the transmitter end, the stream encryptor and stream decryptor(s) each having a pseudo-random generator which generates a variable key which is identical at the transmitter and at the receiver ends with the aid of a secret key,

wherein the variable key depends, moreover, on the state of a state automaton which is allocated to the stream encryptor and to the at least one stream decryptor and which is advanced from ATM cell to ATM cell.

5. The method as recited in Claim 4,

wherein the advance of the state automaton to be derived in response to the detection of a cell boundary by comparing a check sequence computed from the header to a check sequence which is also transmitted in the header of the cell.

6. The method as recited in Claim 4 or 5,

wherein an input variable for the respective pseudo-random generator is generated from the secret key and the respective state with the aid of a predefined function.

7. The method as recited in one of the Claims 4 through 6, several receivers which each have a stream decryptor being connected to the transmission channel, and headers of the ATM cells containing information on which receivers are the destinations of the ATM cells,

wherein the secret key of the stream decryptor at the respective destination is taken as the basis for generating the variable key in the stream encryptor, and the state automatons allocated to the stream encryptor and to the stream decryptors are advanced in response to each transmitted ATM cell.

Abstract

In a device and a method for synchronizing at least one stream decryptor connected to a transmission channel for ATM cells at the receiver end, having a stream encryptor arranged in the transmission channel at the transmitter end, the stream encryptor and stream decryptor(s) each having a pseudo-random generator which generates a variable key which is identical at the transmitter and at the receiver ends with the aid of a secret key, the stream encryptor and the at least one stream decryptor are each allocated a device for cell boundary detection and a state automaton, it being possible for the state automaton to be advanced by the device for cell boundary detection, and the respective state, besides the secret key, being used for generating the variable key.

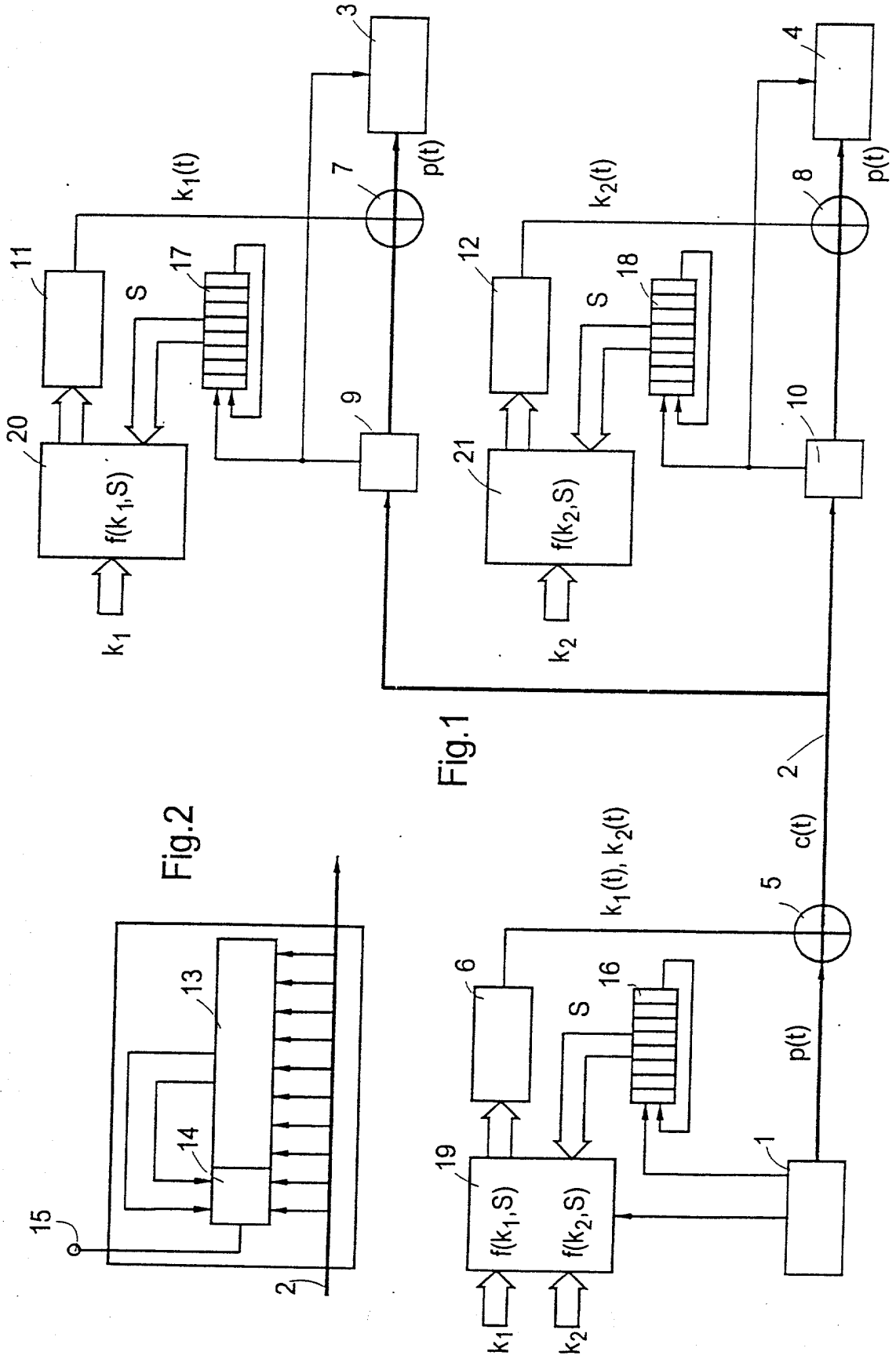
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
S
p(t)
c(t)
$k_1(t)$
$k_2(t)$
$k_1(t), k_2(t)$
k_1
k_2
$f(k_1,S)$
$f(k_2,S)$

Fig.1

Fig.2

P98116 US

DECLARATION AND POWER OF ATTORNEY

Docket No.:520.1002

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter that is claimed and for which a patent is sought on the invention entitled:

DEVICE AND METHOD FOR SYNCHRONIZING VOLTAGE CIPHERING MACHINE IN ATM NETWORKS,

the specification of which (check one)

☐ is attached hereto

☒ was filed on December 9, 1999 as International Application Serial No. PCT/EP99/09844 and was amended on (if applicable).

☐ I hereby authorize and request our attorneys, Davidson, Davidson & Kappel, LLC of 485 Seventh Avenue, New York, New York 10018 to insert here in parentheses (application number _____, filed _____) the filing date and application number of said application when known.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information that is known to me to be material to the patentability of this application as defined in Title 37, Code of Federal Regulations, §1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign and/or provisional application(s) for patent or inventor's certificate listed below and have also identified below any foreign and/or provisional application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

PRIOR APPLICATION(S)

199 01 666.6 Number	Germany Country	18 January 1999 Day/Month/Year Filed	Priority claimed ☒ Yes ☐ No
 Number	 Country	 Day/Month/Year Filed	Priority claimed ☐ Yes ☐ No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial Number	Day/Month/Year Filed	Status
Application Serial Number	Day/Month/Year Filed	Status

And I hereby appoint Clifford M. Davidson, Reg. No. 32,728, Leslye B. Davidson, Reg. No. 38,854, Cary S. Kappel, Reg. No. 36,561, William C. Gehris, Reg. No. 38,156, Morey B. Wildes, Reg. No. 36,968, Robert J. Paradiso, Reg. No. 41,240, Erik R. Swanson, Reg. No. 40,833, Thomas P. Canty, Reg. No. 44,586, and all other registered attorneys and agents at Davidson, Davidson & Kappel, LLC, U.S. Patent and Trademark Office Customer Number 23280, my attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith; correspondence address: DAVIDSON, DAVIDSON & KAPPEL, LLC, 485 Seventh Avenue, 14th Floor, New York, New York 10018; Telephone: (212) 736-1940; Fax: (212) 736-2427.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of sole or first Inventor	Ulrich HEISTER	Full name of additional Inventor	
Inventor's signature	x Ulrich Heister	Inventor's signature	
Date	x 18. June 2001	Date	
Residence	Dieburg, Germany	Residence	
Post Office Address	Waldstrasse 63a D-64807 Dieburg, Germany	Post Office Address	
Citizenship	German	Citizenship	